

日 本 国 特 許 庁
JAPAN PATENT OFFICE

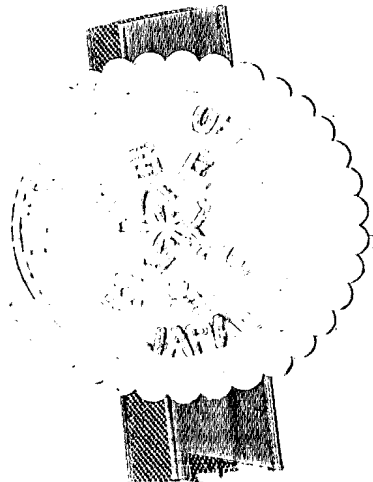
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 1 月 2 1 日
Date of Application:

出 願 番 号 特 願 2 0 0 4 - 0 1 3 4 0 1
Application Number:
[ST. 10/C] : [J P 2 0 0 4 - 0 1 3 4 0 1]

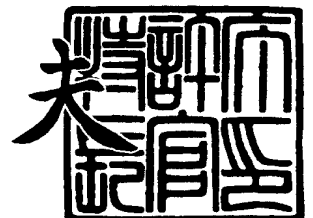
出 願 人 シャープ株式会社
Applicant(s): 田中 初一



特許庁長官
Commissioner,
Japan Patent Office

2 0 0 4 年 2 月 2 5 日

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 1 3 5 1 8

【書類名】 特許願
【整理番号】 03J05215
【提出日】 平成16年 1月21日
【あて先】 特許庁長官 殿
【国際特許分類】 H04L 9/02
H04L 9/14
G06F 7/72
G09C 1/00

【発明者】
【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内
【氏名】 今井 繁規

【発明者】
【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内
【氏名】 永井 知幸

【発明者】
【住所又は居所】 兵庫県神戸市須磨区中落合 4 丁目 2 - 4 6 7 - 3 0 2
【氏名】 田中 初一

【特許出願人】
【識別番号】 000005049
【氏名又は名称】 シャープ株式会社

【特許出願人】
【識別番号】 503034629
【氏名又は名称】 田中 初一

【代理人】
【識別番号】 100080034
【弁理士】
【氏名又は名称】 原 謙三
【電話番号】 06-6351-4384

【選任した代理人】
【識別番号】 100113701
【弁理士】
【氏名又は名称】 木島 隆一

【選任した代理人】
【識別番号】 100116241
【弁理士】
【氏名又は名称】 金子 一郎

【先の出願に基づく優先権主張】
【出願番号】 特願2003- 16761
【出願日】 平成15年 1月24日

【手数料の表示】
【予納台帳番号】 003229
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0316194

【書類名】 特許請求の範囲

【請求項 1】

2つの素数 p , q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s , t と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1 , g_2 を公開鍵として生成する鍵生成手段と、

入力された平文 m に対して、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 , r_2 を用いて、下記の関係式 (3), (4) で表される暗号文 $C = (C_1, C_2)$ を生成する暗号化演算手段とを備えたことを特徴とする暗号化装置。

$$g_1 = g^s (p-1) \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t (q-1) \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

(ただし、 $\text{gcd}\{s, q-1\} = 1$ 、 $\text{gcd}\{t, p-1\} = 1$ とする)

【請求項 2】

素数 p , q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成する鍵生成手段と、

入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成する暗号化演算手段とを備えたことを特徴とする暗号化装置。

$$g_1 = g^s (p-1) \pmod{n} \quad \dots\dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots\dots (3)'$$

(ただし、情報 $b = \text{size of } p \text{ (bits)}$ であって、 $0 < m < 2^{b-1}$ 、 $\text{gcd}\{s, q-1\} = 1$ とする)

【請求項 3】

上記暗号文 C に下記の関係式で示される e を加えて、 $C = (C_1, C_2, e)$ とすることを特徴とする請求項 1 に記載の暗号化装置。

(ただし、 $e = h(d)$ (h は一方向性ハッシュ関数)、 $d = (C_1 + C_2) / m \pmod{n}$ 、 $C_1 = m \cdot g_1^{r_1} \pmod{n}$ 、 $C_2 = m \cdot g_2^{r_2} \pmod{n}$ とする。)

【請求項 4】

上記暗号文 C の乱数部分の計算を行ったデータを蓄積したデータベースを備えていることを特徴とする請求項 1 または 3 に記載の暗号化装置。

【請求項 5】

上記暗号化演算手段は、最初の平文 m_1 だけを暗号文 $C_1 = (C_{11}, C_{12})$ に暗号化し、それ以降の暗号文については、受信した平文 m_i と、平文 m_1 のビット情報と、暗号文 C_1 に含まれる 2つの乱数 R_1 または R_2 とを使用して暗号文を作成することを特徴とする請求項 1 または 3 に記載の暗号化装置。

【請求項 6】

2つの素数 p , q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s , t と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1 , g_2 を公開鍵として用いるとともに、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 , r_2 を用いて、下記の関係式 (3), (4) で表される平文 m を暗号化した暗号文 $C = (C_1, C_2)$ を受信し、

フェルマーの小定理を用いて下記の関係式 (5), (6) で表される受信暗号文 a , b を生成し、該受信暗号文 a , b から、中国人剰余定理を用いて、下記の関係式 (7) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えていることを特徴とする復号化装置。

$$g_1 = g^s (p-1) \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t (q-1) \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r^2} \pmod{n} \quad \dots \dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots \dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots \dots (6)$$

$$m = a A_q + b B_p \pmod{n} \quad \dots \dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $A_q \pmod{p} = 1$ 、 $B_p \pmod{q} = 1$ とする)

【請求項 7】

素数 p 、 q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成し、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を受信し、

フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えていることを特徴とする復号化装置。

$$g_1 = g^{s \cdot (p-1)} \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

$$m = C \pmod{p} \quad \dots \dots (8)$$

(ただし、 $\gcd\{s, q-1\} = 1$ とする)

【請求項 8】

2つの素数 p 、 q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s 、 t と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1)、(2) で表される g_1 、 g_2 を公開鍵として生成する鍵生成手段と、入力された平文 m に対して、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 、 r_2 を用いて、下記の関係式 (3)、(4) で表される暗号文 C_1 、 C_2 を生成する暗号化演算手段とを備えた暗号化装置と、

上記暗号化装置で算出された暗号文 C_1 、 C_2 を受信し、フェルマーの小定理を用いて下記の関係式 (5)、(6) で表される受信暗号文 a 、 b を生成し、該受信暗号文 a 、 b から、中国人剰余定理を用いて、下記の関係式 (7) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えている復号化装置とを備えていることを特徴とする暗号システム。

$$g_1 = g^{s \cdot (p-1)} \pmod{n} \quad \dots \dots (1)$$

$$g_2 = g^{t \cdot (q-1)} \pmod{n} \quad \dots \dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots \dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots \dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots \dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots \dots (6)$$

$$m = a A_q + b B_p \pmod{n} \quad \dots \dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $A_q \pmod{p} = 1$ 、 $B_p \pmod{q} = 1$ とする)

【請求項 9】

素数 p 、 q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成する鍵生成手段と、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成する暗号化演算手段とを有する暗号化装置と、

上記暗号化装置から暗号文 C を受信し、フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行う復号化演算手段とを有する復号化装置とを備えていることを特徴とする暗号システム。

$$g_1 = g^{s \cdot (p-1)} \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

$$m = C \pmod{p} \quad \dots \dots (8)$$

(ただし、 $\gcd\{s, q-1\} = 1$ とする)

【請求項10】

2つの素数 p, q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s, t と、整数に $\bmod n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1, g_2 を公開鍵として生成するとともに、

入力された平文 m に対して、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1, r_2 を用いて、下記の関係式 (3), (4) で表される暗号文 C_1, C_2 を生成することを特徴とする暗号化方法。

$$g_1 = g^s \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ とする)

【請求項11】

素数 p, q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に $\bmod n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成するとともに、

入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成することを特徴とする暗号化方法。

$$g_1 = g^s \pmod{n} \quad \dots\dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots\dots (3)'$$

(ただし、情報 $b = \text{size of } p \text{ (bits)}$ であって、 $0 < m < 2^{b-1}$ 、 $\gcd\{s, q-1\} = 1$ とする)

【請求項12】

2つの素数 p, q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s, t と、整数に $\bmod n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1, g_2 を公開鍵として用いるとともに、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1, r_2 を用いて、下記の関係式 (3), (4) で表される平文 m を暗号化した暗号文 $C = (C_1, C_2)$ を受信し、

フェルマーの小定理を用いて下記の関係式 (5), (6) で表される受信暗号文 a, b を生成し、該受信暗号文 a, b から、中国人剰余定理を用いて、下記の関係式 (7) を満たす平文 m を導出し、復号化処理を行うことを特徴とする復号化方法。

$$g_1 = g^s \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots\dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots\dots (6)$$

$$m = aAq + bBp \pmod{n} \quad \dots\dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $Aq \pmod{p} = 1$ 、 $Bp \pmod{q} = 1$ とする)

【請求項13】

素数 p, q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に $\bmod n$ の演算を施して得られる乗法群の最大生成源 g を用いて下記の関係式 (1) で表される g_1 とを公開鍵として生成し、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を受信し、

フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行うことを特徴とする復号化方法。

$$g_1 = g^s \pmod{n} \quad \dots\dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots\dots (3)'$$

$$m = C \pmod{p} \dots\dots\dots (8)$$

(ただし、 $\gcd\{s, q-1\} = 1$ とする)

【書類名】明細書

【発明の名称】暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法

【技術分野】**【0001】**

本発明は、インターネット等を通じて送受信される通信文を暗号化するための暗号化装置、および暗号化された通信文を復号化するための復号化装置、並びにこれらを備えた暗号システムに関するものである。

【背景技術】**【0002】**

従来より、インターネット等を通じてやり取りが行われるデータ等の漏洩、改竄が問題となっており、この対策として、データ等を暗号化して相手先へ送信する暗号システムが利用されている。

【0003】

暗号システムは、共通鍵暗号方式と公開鍵暗号方式とに大別され、鍵管理の容易性、データ漏洩の危険性が低い等の理由から、主として、公開鍵暗号方式が採用されている。

【0004】

公開鍵暗号方式の代表的な例としては、RSA暗号化方式がある。

【0005】

このRSA暗号化方式は、2つの素数 p 、 q を実質的な秘密鍵として生成し、その積 $n = p q$ を公開鍵の一つとして用いることで、 $p q$ から n は容易に求められるが、 n から2つの素数 p 、 q を求めることが非常に困難であるという性質を利用した公開鍵暗号方式である。

【0006】

このように、 n を公開鍵の一つとして公開することで、誰もが暗号文を作成できる一方、これを復号するために2つの大きな素数 p 、 q を求めることは非常に困難であることから、RSA暗号化方式によって送信されるデータの安全性は非常に高いといえる。

【特許文献1】特開平8-251155号公報（1996年9月27日公開）

【特許文献2】特開2000-214777号公報（2000年8月4日公開）

【発明の開示】**【発明が解決しようとする課題】****【0007】**

しかしながら、上述のような従来のRSA暗号化方式では、データの秘匿性の面では高い性能を有し、アルゴリズムも単純であるものの、その安全性は大きな二つの素数 p 、 q の積 n を素因数分解する困難さに起因している。このため、 $n = p q$ の値を10進法で200桁程度の大きさにする必要があり、暗号化および復号を実行するために必要な n を法とするべき乗計算の実行が極めて困難であるという問題を有している。

【0008】

さらに、RSA暗号化方式は、乗法特性を有しており、2つの署名から第3の署名が生成できるため、安全性の面で問題がある。

【0009】

本発明は、上記の問題点に鑑みてなされたものであり、その目的は、極めて簡単な秘密暗号系を提案し、RSA暗号化方式と等価な安全性を保持しつつ、アルゴリズムをより単純化し、簡単な計算で暗号化および復号化が可能な暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法を提供することにある。

【課題を解決するための手段】**【0010】**

本発明の暗号化装置は、上記の課題を解決するために、2つの素数 p 、 q を秘密鍵として生成し、その積 $n = p q$ と、2つの乱数 s 、 t と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式（1）、（2）で表される g_1 、 g_2

を公開鍵として生成する鍵生成手段と、入力された平文 m に対して、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1, r_2 を用いて、下記の関係式 (3)、(4) で表される暗号文 $C = (C_1, C_2)$ を生成する暗号化演算手段とを備えたことを特徴としている。

$$g_1 = g^s \pmod{n} \quad \dots \dots (1)$$

$$g_2 = g^t \pmod{n} \quad \dots \dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots \dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots \dots (4)$$

(ただし、 $\text{gcd}\{s, q-1\} = 1$ 、 $\text{gcd}\{t, p-1\} = 1$ とする)。

【0011】

上記の構成によれば、公開鍵として生成した鍵 g_1, g_2 は、それぞれ $(p-1)$ 、 $(q-1)$ のべき乗を含んでおり、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて生成した暗号文 C_1, C_2 も、 $(p-1)$ 、 $(q-1)$ のべき乗をそれぞれ含んでいるため、この暗号文 C_1, C_2 を復号化する場合において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、簡単に復号化することができる。

【0012】

すなわち、本発明の暗号化装置は、鍵生成手段により、2つの大きな素数 p, q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s, t とを用いて、それぞれ $(p-1)$ 、 $(q-1)$ のべき乗を含むように公開鍵 $\{g_1, g_2\}$ を生成している。

【0013】

これにより、2つの大きな素数 p, q をそのまま秘密鍵として用いることができ、さらに、公開鍵 $\{g_1, g_2\}$ についても、乱数を用いて、 $(p-1)$ のべき乗を含む非常に簡単な計算で算出できる。

【0014】

また、本発明の暗号化装置の暗号化演算手段によって生成された暗号文は、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、 $(p-1)$ 、 $(q-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【0015】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 $\text{mod } p$ の演算を施すことでその剰余を「1」に帰着させることができる。よって、暗号文 C_1, C_2 から、フェルマーの小定理を用いて、暗号文 C_1, C_2 に対応する2つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、2つの受信暗号文から平文 m を復号化できる。

【0016】

本発明の暗号化装置では、以上のように、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いて簡単に計算できるため、従来の暗号化方式と比較して、高速処理が可能になる。

【0017】

一方、本発明の暗号化装置における安全性については、公開鍵 $\{g_1, g_2\}$ には、それぞれ乱数 s, t が含まれているため、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n は互いに関係が断ち切られている。

【0018】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【0019】

本発明の暗号化装置は、上記の課題を解決するために、素数 p, q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成する

鍵生成手段と、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成する暗号化演算手段とを備えたことを特徴としている。

$$g_1 = g^s \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

(ただし、情報 $b = \text{size of } p \text{ (bits)}$ であって、 $0 < m < 2^{b-1}$, $\text{gcd}\{s, q-1\} = 1$ とする)

上記の構成によれば、公開鍵として生成した鍵 g_1 は、 $(p-1)$ のべき乗を含んでおり、公開鍵 g_1 及び秘密鍵 n を用いて生成した暗号文 C も、 $(p-1)$ のべき乗を含んでいるため、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、この暗号文 C を簡単に復号化することができる。

【0020】

すなわち、本発明の暗号化装置は、鍵生成手段により、2つの大きな素数 p , q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s , t とを用いて、それぞれ $(p-1)$ のべき乗を含むように公開鍵 g_1 を生成している。

【0021】

さらに、秘密鍵 p のサイズ b との関係において、メッセージ m に長さの制限を課し、このサイズ b を用いることで、暗号文の生成および復号化の計算をそれぞれ1つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により暗号化復号化処理を行うことができる。

【0022】

また、本発明の暗号化装置の暗号化演算手段によって生成された暗号文は、上記と同様に、公開鍵 g_1 及び秘密鍵 n を用いて、 $(p-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【0023】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 $\text{mod } p$ の演算を施すことでその剰余を「1」に帰着させることができる。

【0024】

よって、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 g_1 を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の暗号化方式と比較して、さらに高速処理が可能になる。

【0025】

一方、本発明の暗号化装置における安全性については、公開鍵 g_1 には、乱数 s が含まれているため、公開鍵 g_1 及び秘密鍵 n は互いに関係が断ち切られている。

【0026】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、平文 m の長さに制限を加えることで、さらに計算量を減らして暗号化、復号化処理の高速化を実現できる。

【0027】

上記暗号文 C に下記の関係式で示される e を加えて、 $C = (C_1, C_2, e)$ とすることがより好ましい。(ただし、 $e = h(d)$ (h は一方向性ハッシュ関数)、 $d = (C_1 + C_2) / m \pmod{n}$ 、 $C_1 = m \cdot g_1^{r-1} \pmod{n}$ 、 $C_2 = m \cdot g_2^{r-2} \pmod{n}$ とする)。

【0028】

これにより、暗号文 C が長くなるが、メッセージ m が少しでも変わると e が一致なくなるため、適応型選択暗号文攻撃 (CCA2) に対しても耐性を持たせて、より信頼度の高い暗号システムを得ることができる。

【0029】

また、 e はハッシュ関数を用いて計算されているため、32bitsまたは64bits程度の

情報量にまとめることができる。

【0030】

上記暗号文Cの乱数部分の計算を行ったデータを蓄積したデータベースを備えていることがより好ましい。

【0031】

これにより、例えば、暗号文Cに含まれる乱数部分のデータを蓄積した2行f列のデータベースを予め用意しておくことで、暗号化処理を行う際には、このデータベースから対応する乱数を取り出して暗号文を作成することができるため、暗号化処理をより高速化できる。

【0032】

よって、例えば、従来のRSA暗号方式と比較して、計算量を減らして暗号化処理を高速化できるとともに、復号化処理についてもmod pの演算を施すだけで復号化できるため、計算量が多い従来のRSA暗号化方式の暗号システムと比較してはるかに高速化できる。

【0033】

上記暗号化演算手段は、最初の暗号文Cだけを暗号文 C_1 、 C_2 に暗号化し、それ以降の暗号文については前の暗号文 C_1 と、 C_1 に含まれる2つの乱数とを使用して暗号文を作成することがより好ましい。

これにより、最初の暗号文Cについてのみ通常の手順で暗号文を作成し、それ以降の暗号文については、最初のビット $b_i = 0$ の場合には、乱数部分 R_1 を加算し、最初のビット $b_i = 1$ の場合には、乱数部分 R_2 を加算していくことで、暗号文Cを作成できる。

【0034】

本発明の復号化装置は、上記の課題を解決するために、2つの素数 p 、 q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s 、 t と、整数にmod nの演算を施して得られる乗法群の最大生成元 g とを用いて下記の関係式(1)、(2)で表される g_1 、 g_2 を公開鍵として用いるとともに、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 、 r_2 を用いて、下記の関係式(3)、(4)で表される平文 m を暗号化した暗号文 $C = (C_1, C_2)$ を受信し、フェルマーの小定理を用いて下記の関係式(5)、(6)で表される受信暗号文 a 、 b を生成し、該受信暗号文 a 、 b から、中国人剰余定理を用いて、下記の関係式(7)を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えていることを特徴としている。

$$g_1 = g^{s(p-1)} \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^{t(q-1)} \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots\dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots\dots (6)$$

$$m = aAq + bBp \pmod{n} \quad \dots\dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $Aq \pmod{p} = 1$ 、 $Bp \pmod{q} = 1$ とする)。

【0035】

上記の構成によれば、公開鍵として生成した鍵 g_1 、 g_2 は、それぞれ $(p-1)$ 、 $(q-1)$ のべき乗を含んでおり、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて生成した暗号文 C_1 、 C_2 も、 $(p-1)$ 、 $(q-1)$ のべき乗をそれぞれ含んでいるため、この暗号文 C_1 、 C_2 を復号化する際において、フェルマーの小定理($a^{p-1} \equiv 1 \pmod{p}$)を用いて、簡単に復号化することができる。

【0036】

すなわち、本発明の復号化装置が受信する暗号文は、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、 $(p-1)$ 、 $(q-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【0037】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 \pmod{p} の演算を施すことでその剰余を「1」に帰着させることができる。よって、暗号文 C_1 、 C_2 から、フェルマーの小定理を用いて、暗号文 C_1 、 C_2 に対応する2つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、2つの受信暗号文から平文 m を復号化できる。

【0038】

以上のように、本発明の復号化装置では、フェルマーの小定理を用いて簡単に暗号文を復号化できるため、従来の復号化方式と比較して、高速処理が可能になる。

【0039】

本発明の復号化装置は、上記の課題を解決するために、素数 p 、 q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成し、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を受信し、

フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えていることを特徴としている。

$$g_1 = g^{s \cdot (p-1)} \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

$$m = C \pmod{p} \quad \dots \dots (8)$$

(ただし、 $\gcd\{s, q-1\} = 1$ とする)。

【0040】

上記の構成によれば、公開鍵 g_1 を用いて生成した暗号文 C は、 $(p-1)$ のべき乗を含んでいるため、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、この暗号文 C を簡単に復号化することができる。

【0041】

すなわち、本発明の復号化装置は、秘密鍵 p のサイズ b との関係において、メッセージ m に長さの制限を課し、このサイズ b を用いることで、暗号文 C の生成および復号化の計算をそれぞれ1つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【0042】

また、本発明の復号化装置で復号化される暗号文は、公開鍵 g_1 を用いて、 $(p-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【0043】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 \pmod{p} の演算を施すことでその剰余を「1」に帰着させることができる。

【0044】

よって、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 g_1 及び秘密鍵 n を生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【0045】

なお、本発明は、暗号鍵の配布に適用することが可能である。

【0046】

本発明の暗号システムは、上記の課題を解決するために、2つの素数 p 、 q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s 、 t と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1)、(2) で表される g_1 、 g_2 を公開鍵として生成する鍵生成手段と、入力された平文 m に対して、上記公開鍵 $\{g_1$

, g_2 }、秘密鍵 n および乱数 r_1 , r_2 を用いて、下記の関係式 (3), (4) で表される暗号文 C_1 , C_2 を生成する暗号化演算手段とを備えた暗号化装置と、上記暗号化装置で算出された暗号文 C_1 , C_2 を受信し、フェルマーの小定理を用いて下記の関係式 (5), (6) で表される受信暗号文 a , b を生成し、該受信暗号文 a , b から、中国人剰余定理を用いて、下記の関係式 (7) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を備えている復号化装置とを備えていることを特徴としている。

$$g_1 = g^s (p-1) \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t (q-1) \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots\dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots\dots (6)$$

$$m = a A q + b B p \pmod{n} \quad \dots\dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $A q \pmod{p} = 1$ 、 $B p \pmod{q} = 1$ とする)。

【0047】

上記の構成によれば、暗号化装置において、公開鍵として生成した鍵 g_1 , g_2 は、それぞれ $(p-1)$, $(q-1)$ のべき乗を含んでおり、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて生成した暗号文 C_1 , C_2 も、 $(p-1)$, $(q-1)$ のべき乗をそれぞれ含んでいるため、復号化装置において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、暗号文 C_1 , C_2 を簡単に復号化することができる。

【0048】

すなわち、本発明の暗号システムは、暗号化装置と復号化装置とを備えている。暗号化装置は、鍵生成手段を備え、2つの大きな素数 p , q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s , t とを用いて、それぞれ $(p-1)$, $(q-1)$ のべき乗を含むように公開鍵 $\{g_1, g_2\}$ を生成している。

【0049】

これにより、2つの大きな素数 p , q をそのまま秘密鍵として用いることができ、さらに、公開鍵 $\{g_1, g_2\}$ についても、乱数を用いて、 $(p-1)$ のべき乗を含む非常に簡単な計算で算出できる。

【0050】

また、本発明の暗号システムの暗号化装置は、暗号化演算手段において、公開鍵 $\{g_1, g_2\}$ を用いて、 $(p-1)$, $(q-1)$ のべき乗を含んだ式で表される暗号文 C を作成するため、その暗号文 C の復号化にフェルマーの小定理を用いることが可能になる。

【0051】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 \pmod{p} の演算を施すことでその剰余を「1」に帰着させることができる。よって、暗号文 C_1 , C_2 から、フェルマーの小定理を用いて、暗号文 C_1 , C_2 に対応する2つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、2つの受信暗号文から平文 m を復号化できる。

【0052】

以上のように、本発明の暗号システムでは、暗号化装置において、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を生成し、暗号文も簡単な計算で算出でき、さらに、復号化装置において、フェルマーの小定理を用いて簡易に暗号文を復号化できるため、従来の暗号システムと比較して、高速処理が可能になる。

【0053】

一方、本発明の暗号システムにおける安全性については、暗号化装置において作成される公開鍵 $\{g_1, g_2\}$ には、それぞれ乱数 s , t が含まれているため、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n は互いに関係が断ち切られている。

【0054】

よって、本発明の暗号システムによれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【0055】

本発明の暗号システムは、上記の課題を解決するために、素数 p 、 q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成する鍵生成手段と、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成する暗号化演算手段とを有する暗号化装置と、上記暗号化装置から暗号文 C を受信し、フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行う復号化演算手段を有する復号化装置とを備えていることを特徴としている。

$$g_1 = g^s \cdot (p-1) \pmod{n} \quad \dots\dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots\dots (3)'$$

$$m = C \pmod{p} \quad \dots\dots (8)$$

(ただし、 $\text{gcd}\{s, q-1\} = 1$ とする)。

【0056】

上記の構成によれば、暗号化装置において、公開鍵 g_1 及び秘密鍵 n を用いて作成された暗号文 C は、 $(p-1)$ のべき乗を含んでいるため、復号化装置において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、この暗号文 C を簡単に復号化することができる。

【0057】

すなわち、本発明の暗号システムは、暗号化装置が備えている鍵生成手段により、2つの大きな素数 p 、 q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s 、 t とを用いて、それぞれ $(p-1)$ のべき乗を含むように公開鍵 g_1 を生成している。

【0058】

さらに、秘密鍵 p のサイズ b との関係において、メッセージ m に長さの制限を課し、このサイズ b を用いることで、暗号文 C の生成および復号化の計算をそれぞれ1つの式で行うことができるため、復号化装置において、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【0059】

また、本発明の暗号システムにおいては、復号化装置において復号化される暗号文が、 $(p-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【0060】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 $\text{mod } p$ の演算を施すことでその剰余を「1」に帰着させることができる。

【0061】

よって、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 g_1 及び秘密鍵 n を生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【0062】

一方、本発明の暗号システムにおける安全性については、公開鍵 g_1 には、乱数 s が含まれているため、公開鍵 g_1 及び秘密鍵 n は互いに関係が断ち切られている。

【0063】

よって、本発明の暗号化装置によれば、高い安全性を維持しつつ、平文 m の長さに制限を加えることで、さらに簡単な計算により暗号化、復号化処理を行って、高速処理を実現できる。

【0064】

本発明の暗号化方法は、上記の課題を解決するために、2つの素数 p , q を秘密鍵として生成し、その積 $n = pq$ と、2つの乱数 s , t と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1 , g_2 を公開鍵として生成するとともに、入力された平文 m に対して、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 , r_2 を用いて、下記の関係式 (3), (4) で表される暗号文 C_1 , C_2 を生成することを特徴としている。

$$g_1 = g^s (p-1) \pmod{n} \quad \dots\dots (1)$$

$$g_2 = g^t (q-1) \pmod{n} \quad \dots\dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots\dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots\dots (4)$$

(ただし、 $\text{gcd}\{s, q-1\} = 1$, $\text{gcd}\{t, p-1\} = 1$ とする)。

【0065】

上記の暗号化方法によれば、公開鍵として生成した鍵 g_1 , g_2 は、それぞれ $(p-1)$, $(q-1)$ のべき乗を含んでおり、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて生成した暗号文 C_1 , C_2 も、 $(p-1)$, $(q-1)$ のべき乗をそれぞれ含んでいるため、この暗号文 C_1 , C_2 を復号化する場合において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、簡単に復号化することができる。

【0066】

すなわち、本発明の暗号化方法は、2つの大きな素数 p , q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s , t とを用いて、それぞれ $(p-1)$, $(q-1)$ のべき乗を含むように公開鍵 $\{g_1, g_2\}$ を生成している。

【0067】

これにより、2つの大きな素数 p , q をそのまま秘密鍵として用いることができ、さらに、公開鍵 $\{g_1, g_2\}$ についても、乱数を用いて非常に簡単な計算により算出できる。

【0068】

また、本発明の暗号化方法によって生成された暗号文は、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、 $(p-1)$, $(q-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能になる。

【0069】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 $\text{mod } p$ の演算を施すことでその剰余を「1」に帰着させることができる。よって、暗号文 C_1 , C_2 から、フェルマーの小定理を用いて、暗号文 C_1 , C_2 に対応する2つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、2つの受信暗号文から平文 m を復号化できる。

【0070】

以上のように、本発明の暗号化方法では、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いて簡単に計算できるため、従来の暗号化方法と比較して、高速処理が可能になる。

【0071】

一方、本発明の暗号化方法における安全性については、公開鍵 $\{g_1, g_2\}$ には、それぞれ乱数 s , t が含まれているため、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n は互いに関係が断ち切られている。

【0072】

よって、本発明の暗号化方法によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【0073】

本発明の暗号化方法は、上記の課題を解決するために、素数 p , q のうち p を秘密鍵と

して生成し、その積 $n = p q$ と、乱数 s と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成するとともに、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を生成することを特徴としている。

$$g_1 = g^s \cdot (p-1) \pmod{n} \quad \dots\dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots\dots (3)'$$

(ただし、情報 $b = \text{size of } p$ (bits) であって、 $0 < m < 2^{b-1}$, $\text{gcd}\{s, p-1\} = 1$ とする)。

【0074】

上記の暗号化方法によれば、公開鍵として生成した鍵 g_1 は、 $(p-1)$ のべき乗を含んでおり、公開鍵 g_1 及び秘密鍵 n を用いて生成した暗号文 C も、 $(p-1)$ のべき乗を含んでいるため、この暗号文 C を復号化する場合において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、簡単に復号化することができる。

【0075】

すなわち、本発明の暗号化方法は、2つの大きな素数 p , q を発生させ、これを秘密鍵として用いるとともに、この秘密鍵 $\{p, q\}$ と乱数 s , t とを用いて、それぞれ $(p-1)$ のべき乗を含むように公開鍵 g_1 を生成している。

【0076】

さらに、秘密鍵 p のサイズ b との関係において、メッセージ m に長さの制限を課し、このサイズ b を用いることで、暗号文の生成および復号化の計算をそれぞれ1つの式で行うことができるため、中国人剰余定理を用いることなく、より簡単な計算により暗号化復号化処理を行うことができる。

【0077】

また、本発明の暗号化方法によって生成された暗号文は、上記の暗号化方法と同様に、公開鍵 g_1 を用いて、 $(p-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【0078】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 $\text{mod } p$ の演算を施すことでその剰余を「1」に帰着させることができる。

【0079】

よって、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 g_1 を生成し、暗号文も簡単な計算で算出でき、さらにこの暗号文の復号化についても、フェルマーの小定理を用いるだけで簡単に計算できるため、従来の暗号化方法と比較して、高速処理が可能になる。

【0080】

一方、本発明の暗号化方法における安全性については、公開鍵 g_1 には、乱数 s が含まれているため、公開鍵 g_1 及び秘密鍵 n は互いに関係が断ち切られている。

【0081】

よって、本発明の暗号化方法によれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【0082】

本発明の復号化方法は、上記の課題を解決するために、2つの素数 p , q を秘密鍵として生成し、その積 $n = p q$ と、2つの乱数 s , t と、整数に $\text{mod } n$ の演算を施して得られる乗法群の最大生成源 g とを用いて下記の関係式 (1), (2) で表される g_1 , g_2 を公開鍵として用いるとともに、上記公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n および乱数 r_1 , r_2 を用いて、下記の関係式 (3), (4) で表される平文 m を暗号化した暗号文 $C = (C_1, C_2)$ を受信し、フェルマーの小定理を用いて下記の関係式 (5), (6) で表される受信暗号文 a , b を生成し、該受信暗号文 a , b から、中国人剰余定理を用いて、下記の関係式 (7) を満たす平文 m を導出し、復号化処理を行うことを特徴としている。

$$g_1 = g^s \pmod{n} \quad \dots \dots (1)$$

$$g_2 = g^t \pmod{n} \quad \dots \dots (2)$$

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots \dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots \dots (4)$$

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots \dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots \dots (6)$$

$$m = a A_q + b B_p \pmod{n} \quad \dots \dots (7)$$

(ただし、 $\gcd\{s, q-1\} = 1$ 、 $\gcd\{t, p-1\} = 1$ 、 $A_q \pmod{p} = 1$ 、 $B_p \pmod{q} = 1$ とする)

上記の復号化方法によれば、公開鍵として生成した鍵 g_1 、 g_2 は、それぞれ $(p-1)$ 、 $(q-1)$ のべき乗を含んでおり、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて生成した暗号文 C_1 、 C_2 も、 $(p-1)$ 、 $(q-1)$ のべき乗をそれぞれ含んでいるため、この暗号文 C_1 、 C_2 を復号化する場合において、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、簡単に復号化することができる。

【0083】

すなわち、本発明の復号化方法においては、暗号文は、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、 $(p-1)$ 、 $(q-1)$ のべき乗を含んだ式で表されているため、その復号化にはフェルマーの小定理を用いることが可能になる。

【0084】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 \pmod{p} の演算を施すことでその剰余を「1」に帰着させることができる。

【0085】

よって、暗号文 C_1 、 C_2 から、フェルマーの小定理を用いて、暗号文 C_1 、 C_2 に対応する2つの受信暗号文を算出し、ここでさらに中国人剰余定理を用いることで、2つの受信暗号文から平文 m を復号化できる。

【0086】

本発明の復号化装置は、以上のように、フェルマーの小定理を用いて簡単に暗号文を復号化できるため、従来の復号化方式と比較して、高速処理が可能になる。

【0087】

本発明の復号化方法は、上記の課題を解決するために、素数 p 、 q のうち p を秘密鍵として生成し、その積 $n = pq$ と、乱数 s と、整数に \pmod{n} の演算を施して得られる乗法群の最大生成元 g とを用いて下記の関係式 (1) で表される g_1 を公開鍵として生成し、入力された平文 m に対して、上記公開鍵 g_1 、秘密鍵 n および乱数 r を用いて、下記の関係式 (3)' で表される暗号文 C を受信し、

フェルマーの小定理を用いて下記の関係式 (8) を満たす平文 m を導出し、復号化処理を行うことを特徴としている。

$$g_1 = g^s \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

$$m = C \pmod{p} \quad \dots \dots (8)$$

(ただし、 $\gcd\{s, q-1\} = 1$ とする)

上記の復号化方法によれば、公開鍵 g_1 及び秘密鍵 n を用いて生成した暗号文 C は、 $(p-1)$ のべき乗を含んでいるため、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、この暗号文 C を簡単に復号化することができる。

【0088】

すなわち、本発明の復号化方法は、秘密鍵 p のサイズ b との関係において、メッセージ m に長さの制限を課し、このサイズ b を用いることで、暗号文 C の生成および復号化の計算をそれぞれ1つの式で行うことができる。このため、中国人剰余定理を用いることなく、より簡単な計算により復号化処理を行うことができる。

【0089】

また、本発明の復号化方法により復号化される暗号文は、公開鍵 g_1 及び秘密鍵 n を用いて、 $(p-1)$ のべき乗を含んだ式で表されるため、その復号化にはフェルマーの小定理を用いることが可能である。

【0090】

フェルマーの小定理は、 $a^{p-1} \equiv 1 \pmod{p}$ で表され、 $(p-1)$ のべき乗を含む数に対して、 \pmod{p} の演算を施すことでその剰余を「1」に帰着させることができる。

【0091】

よって、単純な秘密鍵 $\{p, q\}$ を用いて、簡単な計算で公開鍵 g_1 を生成し、暗号文も簡単な計算で算出でき、さらに暗号文の復号化についても、フェルマーの小定理だけを用いることで簡単に計算できるため、従来の復号化方式と比較して、さらに高速処理が可能になる。

【発明の効果】

【0092】

本発明の暗号化方法、復号化方法を用いた暗号化装置、復号化装置、暗号システムによれば、高い安全性を維持しつつ、計算量を減らして暗号化および復号化の高速処理を行うことが可能になる。

【発明を実施するための最良の形態】

【0093】

〔実施形態1〕

本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法に関する一実施形態について、図1および図2に基づいて説明すれば以下のとおりである。

【0094】

本実施形態の暗号システムは、図2に示すような、基本的な概念に基づいて、メッセージ（平文） m の暗号化および復号化を行う。

【0095】

すなわち、図2に示すように、メッセージ（平文） m に公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、乱数 R を掛けて暗号文 mR を生成し、これを相手先へ送信する。そして、暗号文 mR を受信した者は、秘密鍵 $\{p, q\}$ を用いて乱数 R を「1」に帰着させ、メッセージ m を復号する。

【0096】

本実施形態の暗号システムは、図1に示すように、暗号化装置（暗号化演算手段）11、通信路14、および復号化演算装置（復号化演算手段）15を備えている。

【0097】

さらに、暗号化装置11は、鍵生成部12および暗号化演算装置13を備えている。

【0098】

鍵生成部12は、メッセージ m の暗号化および復号化に使用する公開鍵 $\{g_1, g_2\}$ と秘密鍵 $\{p, q\}$ とをそれぞれ生成する。なお、公開鍵 $\{g_1, g_2\}$ および秘密鍵 p, q の生成については、後段にて詳述する。

【0099】

暗号化演算装置13は、入力されたメッセージ m を公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて暗号文 C_1, C_2 を作成し、通信路14へ出力する。

【0100】

ここで、平文 m は、 m_1, m_2, m_3, \dots からなり、暗号文 C は、平文 m_1 を暗号化した暗号文 C_1 、平文 m_2 を暗号化した暗号文 C_2 、（以降同様）からなる。

【0101】

暗号文 C_1 は2つの乱数 R_1, R_2 を使った暗号文 C_{11} および C_{12} からなる。

【0102】

$C_1 = (C_{11}, C_{12})$

$$C_{11} = m_1 R_1 \pmod{n}$$

$$C_{12} = m_1 R_2 \pmod{n}$$

実際の暗号化の手順としては、まず、最初の平文 m_1 だけを暗号化した暗号文 $C_1 = (C_{11}, C_{12})$ を作成し、それ以降の暗号文の作成については、平文 m_2 と2つの乱数 R_1, R_2 とを使用して暗号文を作成する。

【0103】

【数2】

$$C_2 = m_2 \oplus R_j \quad (j=1 \text{ or } 2)$$

【0104】

但し、 j の値は、 $m_1 = (b_1 b_2 \dots b_k)$ のビット情報 b_1 に依存して決める。以降、 $C_3, C_4 \dots$ についても同様に暗号化する。

【0105】

復号化演算装置15は、通信路14を介して暗号文 C_1, C_2 を受信するとともに、鍵生成部12から秘密鍵 $\{p, q\}$ を受け取って、暗号文 C_1, C_2 からメッセージ m を復号して出力する。

【0106】

このように、公開鍵 $\{g_1, g_2\}$ を用いて、メッセージ m を暗号化して暗号文 C_1, C_2 として送信し、受信した側において、秘密鍵 $\{p, q\}$ を用いて暗号文 C_1, C_2 をメッセージ m に復号化することで、通信路14におけるメッセージ m の漏洩、改竄等の問題の発生を防止して、安全性の高い通信を行うことができる。

【0107】

ここで、本実施形態の暗号システム10によるメッセージ m の暗号化処理および復号化処理について説明すれば以下のとおりである。

【0108】

まず、鍵生成部12による公開鍵 $\{g_1, g_2\}$ の生成について説明する。

【0109】

鍵生成部12は、秘密鍵 $\{p, q\}$ (p, q は大きな素数とする)、その積 $n = pq$ 、 g を整数 $\times \pmod{n}$ の乗法群の最大生成源、 s, t を $\text{gcd}\{s, q-1\} = 1, \text{gcd}\{t, p-1\} = 1$ を満たす乱数とすると、公開鍵 $\{g_1, g_2\}$ を、以下の関係式(1)および関係式(2)で表される乱数として生成する。

$$g_1 = g^s \pmod{n} \quad \dots \dots \dots (1)$$

$$g_2 = g^t \pmod{n} \quad \dots \dots \dots (2)。$$

【0110】

ここで、上記関係式(1)、(2)には、乱数 s, t が含まれているため、 $n = pq$ の式と上記関係式(1)、(2)とは、完全に関係が断ち切られた状態となっている。よって、公開鍵 $\{g_1, g_2\}$ から秘密鍵 $\{p, q\}$ を導き出すためには、2つの大きな素数 p, q の積である「 n 」から素因数分解によって p, q を導き出す必要がある。

【0111】

続いて、暗号化演算装置13による上記関係式(1)および関係式(2)で表される公開鍵 $\{g_1, g_2\}$ を用いたメッセージ m の暗号文の作成について説明する。

【0112】

m をメッセージ(平文) (但し、 $m < n$ とする)、 r_1, r_2 を乱数、暗号文を $C = (C_1, C_2)$ とすると、暗号文 $C = \{C_1, C_2\}$ は、公開鍵 $\{g_1, g_2\}$ 及び秘密鍵 n を用いて、以下に示す式によって表される。

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \quad \dots \dots \dots (3)$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \quad \dots \dots \dots (4)。$$

【0113】

暗号文 C には、上記関係式(3)、関係式(4)に示すように、乱数 g_1, g_2 の乱数 r_1, r_2 が含まれているため、メッセージ m を乱数として相手先に送信できる。

【0114】

なお、上記関係式(3)および関係式(4)の $g_1^{r_1}$, $g_2^{r_2}$ が、図2に示す概念図における乱数Rに相当する。

【0115】

そして、復号化演算装置15による暗号文 C_1 , C_2 からメッセージmへの復号化について説明する。

【0116】

復号化演算手段15は、秘密鍵 $\{p, q\}$ を用いて、暗号文 C_1 , C_2 をメッセージmに復号化する。

【0117】

ここで、本発明の暗号システムでは、メッセージmを復号化する際に、先ず、フェルマーの小定理($a^{p-1} \equiv 1 \pmod{p}$)を用いて、 $(p-1)$ のべき乗が含まれている乱数部分を「1」に帰着させることができるため、以下に示す受信暗号文a, bが生成される。

$$a = C_1 \pmod{p} = m \pmod{p} \quad \dots\dots (5)$$

$$b = C_2 \pmod{q} = m \pmod{q} \quad \dots\dots (6)$$

【0118】

ここで、上記関係式(5)および関係式(6)の右辺について、 $m > p$, $m > q$ であるため、 $m \pmod{p}$ および $m \pmod{q}$ は乱数であり、メッセージmは完全に復号されていない。

【0119】

そこで、本発明の暗号システムでは、上記2つの関係式(5)および関係式(6)に基づいて、中国人剰余定理を用いてメッセージmを復号する。

【0120】

すなわち、中国人剰余定理を用いれば、メッセージmは、上記関係式(5)および関係式(6)に基づいて以下の関係式(7)によって表されるため、復号化されたことがわかる。

$$m = a A_q + b B_p \pmod{n} \quad \dots\dots (7)$$

(ただし、 $A_q \pmod{p} = 1$, $B_p \pmod{q} = 1$ とする)。

【0121】

本発明の暗号システムは、以上のように、フェルマーの小定理を用いて復号化することができるように、 $(p-1)$ 乗、 $(q-1)$ 乗を含むように公開鍵 $\{g_1, g_2\}$ を生成し、復号化の際には、フェルマーの小定理および中国人剰余定理を用いてメッセージmを復号化する。

【0122】

これにより、非常に簡単な計算で公開鍵 $\{g_1, g_2\}$ を生成できるため、極めて簡単な暗号系を提案できる。また、2つの大きな素数p, qをそのまま秘密鍵 $\{p, q\}$ として用いることができる。さらに、フェルマーの小定理と中国人剰余定理とを用いて簡単な計算によりメッセージmを復号できるため、従来のRSA暗号システムと比較して、暗号化する際の計算量を減らして、高速処理が可能な暗号システムを得ることができる。

【0123】

〔実施形態2〕

本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法に関する他の実施形態について説明すれば、以下のとおりである。

【0124】

本実施形態の暗号システムは、上記実施形態1の暗号システムと基本的な原理については同様であるが、秘密鍵pのサイズbをメッセージmとの関係で制限することを条件として、アルゴリズムをより単純化することができる。

【0125】

すなわち、上記実施形態1の暗号システムでは、1つのメッセージmに対して、2つの

暗号文 C_1 , C_2 を生成しているが、本実施形態の暗号システムでは、秘密鍵 p のサイズ b を $0 < m < 2^{b-1}$ という条件式を満たすように制限し、このサイズ b を用いることで、1つの暗号文 C を生成し、これを復号するだけで済むため、より暗号化、復号化処理を高速化が図れる。

【0126】

具体的には、暗号化演算装置は、乱数 r を発生させるとともに、秘密鍵 p のサイズ b と、秘密鍵 p とを用いて下記の関係式 (1) で表される公開鍵 g_1 と、(3)' で表される暗号文 C を生成する。

$$g_1 = g^{s \cdot (p-1)} \pmod{n} \quad \dots \dots (1)$$

$$C = m \cdot g_1^r \pmod{n} \quad \dots \dots (3)'$$

(ただし、メッセージ m とサイズ b とは、 $0 < m < 2^{b-1}$ の条件式を満たす)。

【0127】

続いて、上記暗号文 C の復号化については、上記実施形態 1 の暗号システムと同様に、復号化演算装置が、フェルマーの小定理 ($a^{p-1} \equiv 1 \pmod{p}$) を用いて、下記の関係式 (8) を導出する。

$$m = C \pmod{p} \quad \dots \dots (8)。$$

【0128】

ここで、暗号文 C には、 g_1 が含まれており、実施形態 1 の g_1 の関係式 (1) より、 g_1 は $(p-1)$ 乗を含んでいるため、 \pmod{p} をとることにより、 m 以外の数を 1 に帰着させることができるため、メッセージ m を容易に復号化できる。

【0129】

本実施形態の暗号システムでは、以上のように、秘密鍵 p のサイズ b についてメッセージ m との関係で制限する。そして、公開鍵 g_1 を生成して、1つの暗号文 C を生成し、この暗号文 C を秘密鍵 p を用いて復号するため、実施形態 1 で用いた中国人剰余定理を用いなくても容易に復号化処理を行うことができる。

【0130】

よって、上記実施形態 1 の暗号システムと等価の安全性を維持しつつ、実施形態 1 の暗号化装置よりもさらに高速処理が可能な暗号システムを得ることができる。

【0131】

また、上述した本実施形態の暗号システムは、以下のような特徴を有している。

【0132】

1つ目の特徴としては、暗号文 C_1 , C_2 を示す上記関係式 (3), (4) には、 g_1^{r-1} が含まれているため、メッセージ m を送るたびに暗号文が異なる、いわゆる確率暗号となっている。これは、べき乗の「 r 」が乱数であることによる特徴である。よって、RSA 暗号化方式では、メッセージ m と暗号文 C とが一对一に対応するのに対し、本発明の暗号システムでは、メッセージ m と暗号文 C とが一对一に対応しないため、暗号文 C から解読することが困難であり、より暗号強度を高めることができる。

【0133】

2つ目の特徴としては、メッセージ m から暗号文 C への変換は容易であるが、その逆の変換は非常に困難である、いわゆる一方向性関数であることが挙げられる。

【0134】

3つ目の特徴としては、1つ目の特徴としてあげたように、メッセージ m と暗号文 C とが一对一に対応しないため、生成された暗号文が同じ暗号文 C であっても、元のメッセージが異なるメッセージ m_0 , m_1 である可能性がある。よって、暗号文 C からは、どのメッセージ m を暗号化したものかわかりにくいため、暗号強度を高めることができる。

【0135】

ここでさらに、暗号解析者による以下に示す3種類の攻撃に対する本発明の暗号システムの安全性について説明すれば以下のとおりである。

【0136】

まず、1つ目の攻撃として、選択平文攻撃 (Chosen Plaintext Attack: CPA) に対

する安全性について説明する。

【0137】

この選択平文攻撃は、通常、暗号文を作成する際のプロセスであり、与えられた平文（メッセージ） m に対する暗号文のペアを多数作成し、新しい暗号文が与えられた際に平文を求めることができるか否かについて調べることで、暗号文を復号する鍵を求める攻撃である。

【0138】

これに対し、本発明の暗号システムは、上述のように、一方向性関数であって、かつ確率暗号であるため、メッセージ m と暗号文 C とが一対一に対応していない。このため、この選択平文攻撃に対する本発明の暗号システムの安全性は高いことがわかる。

【0139】

2つ目の攻撃として、非適応型選択暗号文攻撃（Non-Adaptive Chosen Ciphertext Attack: CCA1）に対する安全性について検討する。

【0140】

この非適応型選択暗号文攻撃は、暗号文を与えてこれに対応する平文のペアを作成し、ターゲットとなる暗号文を与えて平文が求められるかを調べる攻撃であって、かつ復号化したいターゲットとなる暗号文に質問した後は一切質問不可となる条件の攻撃である。

【0141】

これに対して、本発明の暗号システムは、上記と同様に、一方向性関数であって、かつ確率暗号であるため、メッセージ m と暗号文 C とが一対一に対応していない。このため、この非適応型選択暗号文攻撃に対する本発明の暗号システムの安全性は高いことがわかる。

【0142】

3つ目の攻撃として、適応型選択暗号文攻撃（Adaptive Chosen Ciphertext Attack: CCA2）に対する安全性について説明する。

【0143】

この適応型選択暗号文攻撃は、暗号文を与えてこれに対応する平文のペアを作成し、ターゲットとなる暗号文を与えて平文が求められるかを調べる攻撃であって、かつ復号化したいターゲットとなる暗号文以外は何をいつ聞いてもよいという条件で、前回の結果を活用して繰り返し処理を行う攻撃である。

【0144】

これに対して、本発明の暗号システムは、ターゲットとなる暗号文が識別不能であるため、完全に安全であるとは言い難い。

【0145】

つまり、ターゲットとなる暗号文 $C = (C_1, C_2)$ とすると、 C_1, C_2 は以下に示すようになる。

$$C_1 = m \cdot g_1^{r_1} \pmod{n} \Rightarrow C_1^* = m \cdot g_1^{r_1 + t_1} \pmod{n}$$

$$C_2 = m \cdot g_2^{r_2} \pmod{n} \Rightarrow C_2^* = m \cdot g_2^{r_2 + t_2} \pmod{n}$$

ここで求めた $C^* = (C_1^*, C_2^*)$ は $C^* \neq C$ であるが、 C^* を提示して平文 m を得ることができるため、本発明の暗号システムは、この適応型選択暗号文攻撃に対しては安全ではないといえる。

【0146】

そこで、本実施形態の暗号システムでは、適応型選択暗号文攻撃に対して耐性を持たせるために、 $C = (C_1, C_2, e)$ とする。

【0147】

ただし、「 e 」は、 $C_1 = m \cdot g_1^{r_1} \pmod{n}$ 、 $C_2 = m \cdot g_2^{r_2} \pmod{n}$ より、 $d = (C_1 + C_2) / m \pmod{n}$ であるから、 $e = h(d)$ （ h は一方向性ハッシュ関数）とする。

【0148】

これにより、暗号文 C は長くなるという問題はあるが、 e を32bitsまたは64bitsに

まとめることができるとともに、メッセージ m が少しでも変わると e が一致しなくなるため、上記適応型選択暗号文攻撃に対して耐性を持たせて、信頼度の高い暗号システムを得ることができる。

【0149】

なお、本発明の暗号システムは、以下に示すデータベースを用いることにより、演算をより高速化できる。

$$DB(2, e) = [R_{ij} = g_i^{r_{ij}} \pmod n]$$

(ただし、 $1 \leq i \leq 2$, $1 \leq j \leq e$)

$$C = (C_1, C_2)$$

【0150】

【数1】

$$C_1 = m \cdot \prod_{k=1}^{\delta_1} R_{1,j_k} \pmod n$$

$$C_2 = m \cdot \prod_{l=1}^{\delta_2} R_{2,j_l} \pmod n$$

【0151】

すなわち、2行× e 列のデータベースに R_{ij} を前もって計算して蓄積しておくことで、暗号化処理を行う際には、このデータベースから R_{ij} を取り出して乱数部分を作ることができるため、暗号化処理をより高速化できる。

【0152】

これにより、例えば、計算量が多い従来のRSA暗号方式と比較して、暗号化処理を高速化できるとともに、復号化処理については $\text{mod } p$ の演算を施すことだけで復号化できるため、計算量が多いRSA暗号化方式と比較してはるかに高速化できる。

【0153】

さらに、本発明の暗号システムは、べき乗の特性を利用して、図3に示すような拡張ブロックサイファに応用することができる。

【0154】

この拡張ブロックサイファは、暗号文 C_1 だけを通常のスキルで暗号文 C_{11} , C_{12} に暗号化し、後の C_2 以降の暗号文については前の暗号文 C_{11} , C_{12} に含まれる2つの乱数 R_1 , R_2 を使用して暗号文を作成するため、従来の共通鍵暗号系と公開鍵暗号系とで処理をより高速化できる。

【0155】

具体的には、最初の暗号文 C_1 についてのみ通常の手順で暗号文 C_{11} , C_{12} を作成し、 C_2 以降の暗号文については、最初のビット $b_i = 0$ の場合には、 R_1 を加算し、最初のビット $b_i = 1$ の場合には、 R_2 を加算していくことで、暗号文 C を作成できる。

【0156】

【表 1】

《暗号化》

	べき乗計算	かけ算
Original	2	2
Extended	$2/k$	$2/k$

単位(回)

《復号化》

	割り算	かけ算
Original	2	2
Extended	$4/k$	$2/k$

単位(回)

【0157】

表1は、図3に示す拡張ブロックサイファによって計算回数をどれだけ減らせるかを示している。

【0158】

暗号化処理については、表1上段に示すように、ブロック長 k とすると、べき乗計算、掛け算ともに、計算回数を $2/k$ 回に減らせることが分かる。

【0159】

復号化処理については、表1下段に示すように、ブロック長 k とすると、割り算については $4/k$ 回に、掛け算については $2/k$ 回に減らせることが分かる。

【0160】

以上のように、本発明の暗号システムの応用例として、拡張ブロックサイファを適用することで、より計算回数の少ない高速処理が可能なハイブリッド型の暗号システムを得ることができる。

【0161】

なお、上記実施形態2の単純化した暗号システムにこの拡張ブロックサイファを適用した場合には、表1に示す計算回数は全て1回になり、非常に使い易い暗号システムが得られる。

【0162】

さらに、本発明の暗号システムをデジタル署名に適応させた場合について説明すれば以下のとおりである。

【0163】

まず、公開鍵 $\{g_1, g_2\}$ の指数部分 $s(p-1)$ と $t(q-1)$ とを α, β とすると、署名 (u, v) は以下の式で表される。

$$u = \alpha r + \beta m \pmod{\Phi(n)} \quad \dots\dots (12)$$

$$v = g^{(\alpha^2 r + \beta^2)} \pmod{n} \quad \dots\dots (13)$$

(ただし、メッセージ m , $m \leq M \leq \Phi(n)$, 乱数 r とする)。

【0164】

上記関係式(12)より、 u には不明な変数が3つ以上あるため、この式を解くことはできない。また、上記関係式(13)より、 v では、 g , α , β , r は全て秘密の変数であるため、この式を解くこともできない。

【0165】

また、この署名付きメッセージ $\{m, (u, v)\}$ の認証式は、以下の関係式で表される。

$$(g_1^m g_2)^u = v^m \pmod{n} \quad \dots\dots (14)。$$

【0166】

続いて、この関係式(14)を認証する。

【0167】

$$\begin{aligned} (g_1^m \cdot g_2)^u &= g^{(\alpha m + \beta)(\alpha r + \beta m)} \pmod{n} \\ &= g^{(\alpha^2 r + \beta^2)m} \pmod{n} \\ &= v^m \pmod{n} \end{aligned}$$

(ただし、 $g^{\alpha\beta} = g^{st(p-1)(q-1)} = g^{st\Phi(n)} = 1 \pmod{n}$ とする)。

【0168】

これにより、署名した人から送信されたメッセージ m であることが認証された。

【0169】

本発明の暗号システムは、以上のように、従来とは異なる新たな方式であって、安全性が高く、高速処理が可能なデジタル署名を提案できる。

【0170】

なお、本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法は、例えば、相手認証、相互認証、電子選挙および電子入札等にも適用することができる。

【0171】

また、本発明の暗号システムは、2つの大きな素数 p , q を秘密鍵として用いるとともに、素数 p , q についてその積 $n = pq$ と、 $(p-1)$ および $(q-1)$ のべき乗および乱数 s , t を含む g_1 , g_2 とを公開鍵 $\{g_1, g_2\}$ 、秘密鍵 n として、暗号文 $C = (C_1, C_2)$ を作成する暗号化装置と、該暗号文 C に対してフェルマーの小定理を用いて暗号文 C を復号化する復号化装置とを備えていることを特徴とする暗号システムと、関係式を用いることなく表現することもできる。

【0172】

なお、本発明の暗号化技術は、例えば、家庭内の小さな領域でのストリーミングデータのスクランブラあるいはデスクランブラに適用することが可能である。

【0173】

また、本発明は、暗号鍵の配布に適用することも可能である。

【0174】

本発明は上述した各実施形態に限定されるものではなく、請求項に示した範囲で種々の変更が可能であり、異なる実施形態にそれぞれ開示された技術的手段を適宜組み合わせて得られる実施形態についても本発明の技術的範囲に含まれる。

【図面の簡単な説明】

【0175】

【図1】本発明の暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法の一実施形態を示す暗号システムの構成を示すブロック図である。

【図2】本発明の暗号化および復号化処理の概念を示すブロック図である。

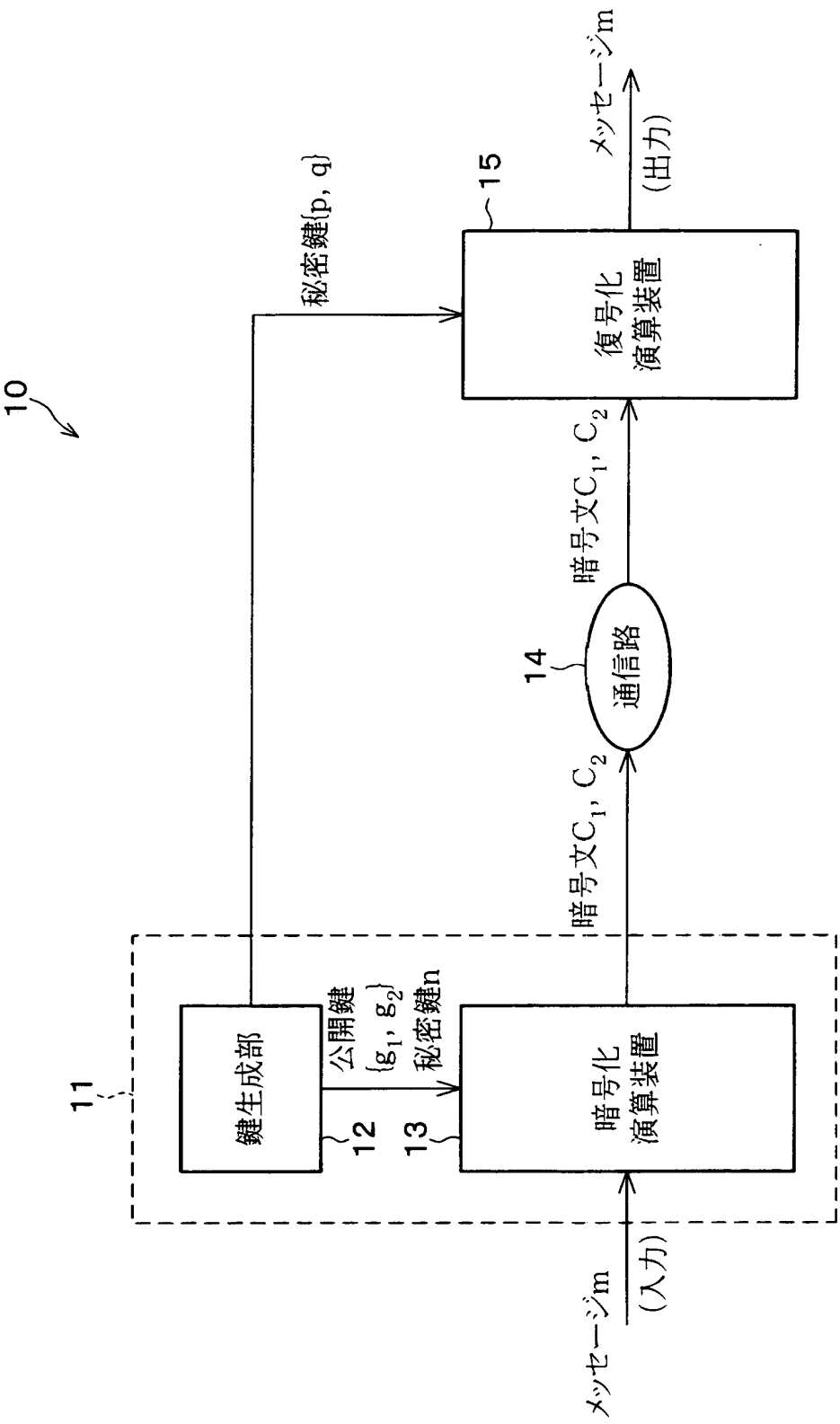
【図3】本発明の暗号システムの応用例としての拡張ブロックサイファの態様を示す図である。

【符号の説明】

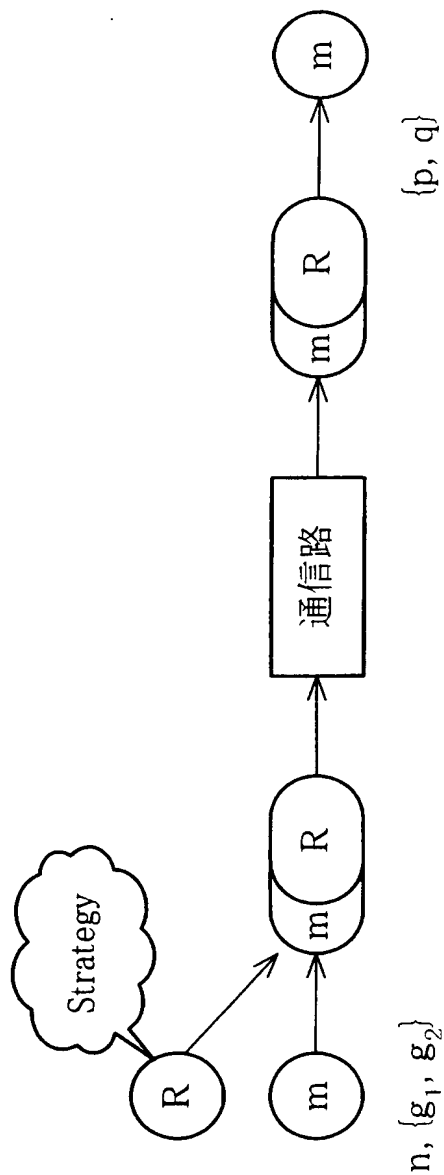
【0176】

10	暗号システム
11	暗号化装置
12	鍵生成部
13	暗号化演算装置
14	通信路
15	復号化演算装置
m	メッセージ（平文）
n	秘密鍵（2つの大きな素数の積）
g_1, g_2	公開鍵
p, q	秘密鍵（2つの大きな素数）
C	暗号文
C_1, C_2	暗号文

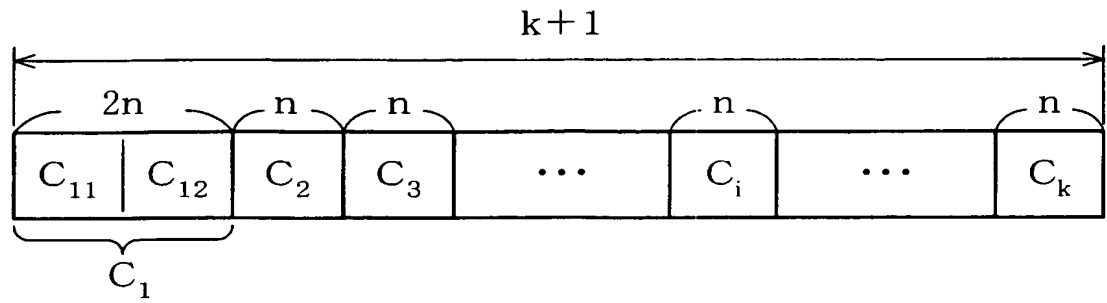
【書類名】 図面
【図 1】



【図 2】



【図 3】



$$C_1 = (C_{11}, C_{12}), \quad C_{11} = m_1 R_1 \pmod{n}, \quad C_{12} = m_1 R_2 \pmod{n}$$

$$C_i = m_i \oplus R_{b_i+1}; \quad b_i = 0 \text{ or } 1 \in m_1, \quad 2 \leq i \leq k < \lfloor \log_2 n \rfloor$$

【書類名】 要約書

【要約】

【課題】 極めて簡単な暗号系を提案し、RSA暗号化方式と等価な安全性を保持しつつ、暗号化および復号化する際の計算量を減らして単純化し、簡単な計算で暗号化および復号化が可能な暗号化装置および復号化装置、並びにこれらを備えた暗号システム、暗号化方法および復号化方法を提供する。

【解決手段】 暗号システム10は、暗号化装置11、通信路14、および復号化演算装置15を備えている。暗号化装置11の鍵生成手段12は、公開鍵 $\{g_1, g_2\}$ を、 $(p-1)$ 、 $(q-1)$ のべき乗を含む乱数として生成し、復号化の際には、フェルマーの小定理および中国人剰余定理を用いてメッセージ m を復号化する。

【選択図】 図1

特願 2 0 0 4 - 0 1 3 4 0 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 0 4 9]

1 . 変更年月日 1 9 9 0 年 8 月 2 9 日

[変更理由] 新規登録

住 所 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号

氏 名 シャープ株式会社

特願 2 0 0 4 - 0 1 3 4 0 1

出 願 人 履 歴 情 報

識別番号

[5 0 3 0 3 4 6 2 9]

1. 変更年月日

2 0 0 3 年 1 月 2 4 日

[変更理由]

新規登録

住 所

兵庫県神戸市須磨区中落合4丁目2-467-302

氏 名

田中 初一